

Multi-model-based Access Control in Construction Projects

Frank Hilbert

TU Dresden

Institute of Construction Informatics
Dresden University of Technology
Dresden, Germany

frank.hilbert@tu-dresden.de

Raimar J. Scherer

TU Dresden

Institute of Construction Informatics
Dresden University of Technology
Dresden, Germany

raimar.scherer@tu-dresden.de

Larissa Araujo

USP

Engineering School of Sao Carlos
University of Sao Paulo
Sao Paulo, Brazil

larissaedaraujo@sc.usp.br

During the execution of large scale construction projects performed by Virtual Organizations (VO), relatively complex technical models have to be exchanged between the VO members. For linking the trade and transfer of these models, a so-called multi-model container format was developed. Considering the different skills and tasks of the involved partners, it is not necessary for them to know all the models in every technical detailing. Furthermore, the model size can lead to a delay in communication. In this paper an approach is presented for defining model cut-outs according to the current project context. Dynamic dependencies to the project context as well as static dependencies on the organizational structure are mapped in a context-sensitive rule. As a result, an approach for dynamic filtering of multi-models is obtained which ensures, together with a filtering service, that the involved VO members get a simplified view of complex multi-models as well as sufficient permissions depending on their tasks.

1 Introduction

For the processing of large and complex construction projects, single independent organizations work together as Virtual Organizations (VO) [1], combining their core competencies [2, 3]. To manage the complexity in construction in which the costs incurred within a project vary, both physical and functional information split into various domain-specific application models (e.g. building model, cost model, time model, etc.) on the basis of which the work is running, typically discipline-specific [4]. The use of Building Information Modelling (BIM) is becoming increasingly important for collaborative processing [5]. The elements of the various specialized models are implicitly linked together (e.g. the component inside wall xy from the model building with the process concrete first floor from the process model). To transfer application models together with their links, in the German Project MEFISTO ¹ and in the international Project HESMOS ², a multi-model container format (MMC) was developed which summarizes application models with their dependencies [6]. When using this MMC approach, however, the following aspects must be considered:

- (A1) The MMC, based on the number and granularity of the application models, becomes relatively large. Because of distributed processing in Virtual Organizations, these multi-models are shared very often and the size of the model can lead to the obstruction of communication (e.g. the size of the IFC building model of a simple high-rise building is about 40 MB).
- (A2) For the processing of individual project tasks only a relatively small part of the subject model is usually interesting. According to their current project responsibilities the agents are only interested, in most cases, in the specific aspects (e.g. building services, building spatial structures, structural analysis, etc.).

¹<http://www.mefisto-bau.de>

²<http://hesmos.eu>

- (A3) It is not necessary, and for reasons of data protection, may also not be desirable that all partners involved must know all the technical details of the project model.

From these considerations, it is useful to facilitate the working with multi-models, the transmitting of model cut-outs or the generating of model views. For this purpose, a central filter and mapping service are currently being developed at the TU Dresden, which generate partial application models while maintaining the link structure between the application models [7]. This filtering service is used within this approach to enforce the definition of model views and covers the aspect of access and privacy when accessing multi models within virtual organizations. In this manner, an initiated approach, as to the integration of these filter services in a context-sensitive fine-grained access control, is described. The next section briefly describes the structure of the multi-model used. On this basis, in Chapter 3, different multi-model filter designs are considered; first the uses of multi-model templates for the generation of model views, and second, the filtering of elementary models for creating cut-outs. Then, in chapter 4, the idea of an extended context-sensitive role model for virtual organizations is pursued, and in chapter 5, a proposed methodology for using this model for the filtered access to multi-models follows. The last chapter outlines practical scenarios and gives an outlook into further development.

2 Basic Concepts

2.1 The multi-model container format

In order to distribute project information together from the various semantically and structurally inhomogeneous domain expert models and, on the other side, externalize the implicit relationship between the model elements, a generic link model was developed, which will be shown together with the associated application models within a multi-model. Then the link model in the form of an XML document is stored, the format of the application models is not specified. The multi-model was changed in a so-called multi-model container (MMC) which is within the multi-model container and separated in each model, described by metadata (see Figure 1). These multi-model containers are read into the specialized applications of the VO partners, modified and shared with other partners. More information about the structure and the use of MMC is given by Fuchs in [6].

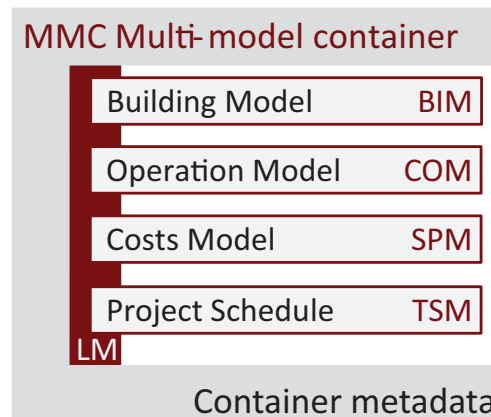


Figure 1: Example Structure of the Multi-Model-Container

2.2 Filter Concepts for Multi-Models

In the filtering of multi-models it is necessary to distinguish between the pure selection of application models as they are defined for model-views (domain-views) with any setting of the desired granularity (see Figure 2) and of the filter model to generate model cut-outs (see Figure 3).

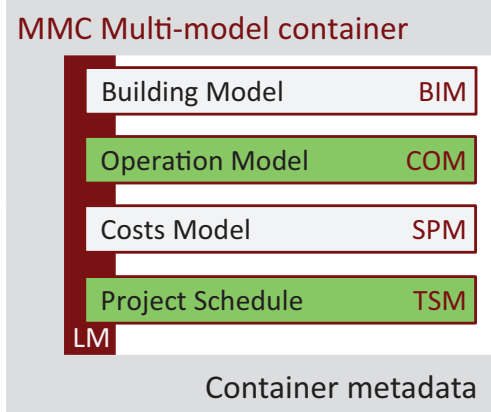


Figure 2: Example of a Multi-Model-View

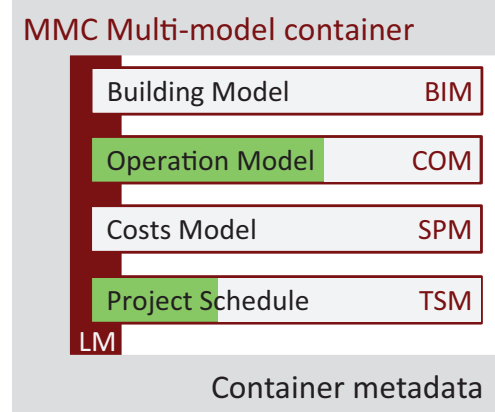


Figure 3: Example of a Multi-Model-Cutout

For handling different tasks, it is often not necessary for all application models to be available. The use of model views serves not only for the simplified representation of complex issues but also to increase the security against unauthorized data access and is achieved by the simplest form of filtering through the use of multi-model templates.

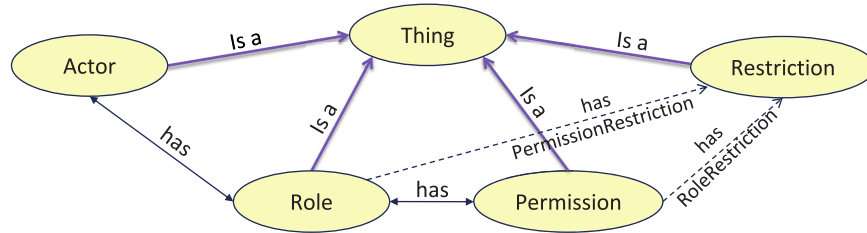


Figure 4: filtering with multi-model templates

In the MEFISTO Project seven exemplary different multi-model templates have been defined which are based on the phases of the project and selected in the first step of each different subset of application models (Building, Operation, Performance, Costs and Construction Site Model). In a second step, the associated link model can be reduced to the remaining links of the tray model elements. Then, the templates demand not only the existence of application models in the multi-model, but claim additionally the compliance model-dependent levels of detail and processing status. It is conceivable that in a production model, the application building model (BM) and operation model (OM) are structured much more comprehensively than within the model range. In a third step, these additional conditions are checked using the metadata within the container. In Table 1, examples of granularities are outlined (e.g. in the application model the process model-column templates of the frame schedule (0.1), coarse schedule (0.2)) to detail schedule (1)). Other various project plans are discussed in more detail in [4].

Project Phase	Task	MM-Template	BM	OM	PM	CM	CSM
Offer phase	Offer request	Tender Model	0,5	0,1	0,1	0	0
Offer phase	Offer delivery	Offer Model	0,5	0,2	1	0,5	0
Contract phase	Negotiation	Negotiation Model	0,5	0,2	1	0,7	0
Contract phase	Commissioning	Contract Model	1	1	1	1	0
Execution phase	Scheduling	Tender Model	1	1	1	1	0,7

Table 1: LOD of Application Models in Multi-model templates

For the selection of individual object fields for further processing or to facilitate semantic multi-model filter, the use of specialized model cut-outs is desirable. Then these excerpts can turn into various, in part dynamic, criteria to be defined, for example as geometric part-models, time periods or (external) object properties of the model elements. The generation of task-specific ad-hoc multi-model views, which are combined to link models of BIM data with information from other application models is relatively complex and is a topic of current research. Katranuschkov describes in [7] an approach for the generation of BIM-based multi-model views, and a reference implementation, based on the use of open IFC toolset from the University of Weimar and HOCHTIEF that, with the use of the generic Model Subset Definition Schema (GMSD), focuses on these goals. Another challenge is the generation of partial geometric models, here under certain circumstances broken up into objects, because it must be generated at different levels of the objects detail. This aspect is the subject of current research within the project HESMOS and is not described in this work.

3 Context-dependent Access Control

Camarinha-Matos differentiated in [8], exogenous and endogenous VO roles, with the former relationships reflecting outwards, such as interaction with the environment, customers, competitors and potential partners, and on the other side endogenous roles which are represented by the relationships within the VO. These endogenous roles handle the VO participants during the exercising of their cooperation and are defined in the VO-initiation, as well as other descriptive attributes, in the Organization Model. The classic role-based access control (RBAC) [9] defines the relationship in a simple way:

WHO (project role) may WHAT (authorizations)?

Hence, VO participants may bring different talents or skills into a VO, so that the VO actors are assigned with so-called potential roles. Both in [10] and in [11], it was found that the role assignment of the VO members is not rigidly fixed in practice, but contextual and dynamic role assignments are subject to restrictions and must therefore be context-dependently modelled and dynamically evaluated. Only with this combination, the observance of the principle of Separation of Duty [9] and the Principle of Least Privilege [12] can be ensured. We use an expanded role model for which the access control including the access context offers and determines illustrated in simplified form:

WHO (current role) may WHAT (authorizations) with WHOM (object) in which SITUATION (context)?

An example scenario: A player is entrusted with the tasks within the VO plan creation and plan evaluation. To ensure the Separation of Duty, this actor should not be allowed to control himself, so both roles can only be selected when accessing different objects.

3.1 The use of context information

To add context-sensitive abilities to security mechanisms, context attributes must be described in a formal context model. The context attributes are not individually described within this context model, but they are assigned real world objects. This so-called deputy approach describes a basic concept for the representation of contextual information [13] and link distributed context attributes of the subject and the object model together with the environment context attributes. Using a context model now we can combine previously individually held context information so that situations can be precisely described. The relevant relationships for access decisions can be complex and involve various types and combinations of context information. For the modelling of the knowledge about their relationships, the impact of this information has to be formally described. For the definition of the access control policies, we use the Web Rule Language (SWRL) (Horrocks et al., 2003) to achieve flexibility and interoperability as well as easy administration. Some examples of SWRL rules:

- Role assignment:
(Actor(?a), Role(?e), Resource(?r), hasTarget(?a,?r), hasRole(?a,?e), hasOwner(?r,?a))
->PermittedRole(?e)
- Ownership:
(Action(?a), Resource(?r), hasTarget(?a,?r), hasActor(?a,?x), hasOwner(?r,?x))
->PermittedAction(?a)
- Sstate dependence:
(Action(?a), Resource(?r), hasTarget(?a,?r), hasObjectRestriction(?a,?x), has-
PassRestriction(?r,?x)) ->PermittedAction(?a)

3.2 Structure of the VO model

We have modelled the RBAC-Model in our VO-Ontology model with the classes Actor, Role, Permission and Restriction. Objects of the Class Restriction define the context sensitive Assignment-Restriction in the form of SWRL-rules. The Relation sr is modelled by the bijective mapping of the ObjectProperty hasActorRoleAssignment and hasRoleActorAssignment, which connect the classes Actor and Role.

Both, the ObjectProperty hasPermissionRoleAssignment and hasRolePermissionAssignment connect the classes Role and Permission and reflect the Relation sr. The SubProperty hasRoleRestriction and hasPermissionRestriction link the Class Restriction to the ObjectProperty hasActorRoleAssignment and hasPermissionRoleAssignment and realize the functions fc(sr) and gc(pr) (in Figure 3 dotted). The Restriction-Objects contain the restrictions to be evaluated, where the Open World Assumption is valid, i.e. the modelled Relations sr and pr are true, if there are no Restrictions or the Restrictions can be evaluated to be true.

3.3 Dynamic Authorization Decisions

Scholz describes in [15] mutual trust as the basis for VOs and the transparent handling of explicit rules and standards as the basis for this confidence. For the rules of a context-based access control for multi-models, we use the Fine Grain Access Control (FGAC) rules described by Franzoni in [16]

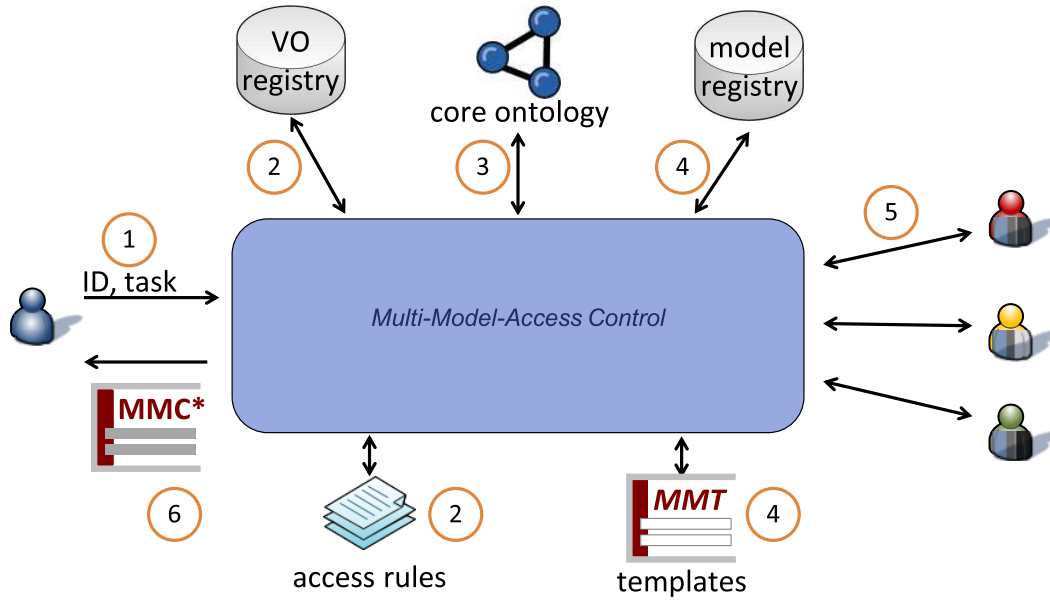


Figure 5: VO Model

with a context-sensitive expansion, which additionally accesses the context in which access decisions are integrated. The actual access role when accessing an object instance from a dynamic access control according to the access context, consists of various determined static (potential roles with permissions) and dynamic conditions (object status and subject status, subject-object relationships and project status). This consists mainly of an empty MMC with pre-populated metadata descriptions. Using these templates it is easy to determine whether a padded MMC corresponds to a template. In MEFISTO a VO-based service platform is used which registers all created MMC templates and the metadata of all transmitted application models.

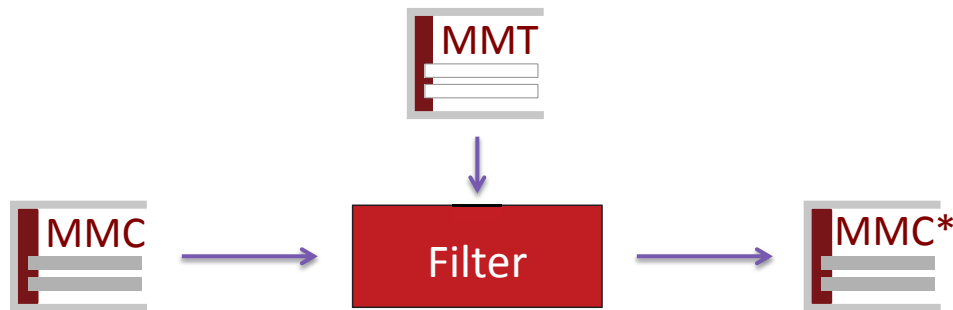


Figure 6: Access Control with Multi-Model-Filter

We propose a context-sensitive access control in 5 steps:

1. The role of a requesting actor is determined by evaluating its potential VO roles and the access context.

2. The User ID is checked in the VO registry and connected access rules are evaluated.
3. With the Task description in the core ontology, the necessary permissions are evaluated
4. The task-dependent Template is searched on the VO-platform. If there is no template, then it will return an unfiltered Multi-Model, according to the preferences, or the access will not be permitted. If there is a template, it is created on the basis of a container template a Multi-Model-Container through the base service. Then, the registered trade models use the service from the platform and search in the model registry for an application model in the desired resolution.
5. If an application model does not exist in the required granularity, the subject-specific model type of filter methods and services are requested and an application model with higher granularity and the desired level of detail are given as an argument. The application model produced is inserted into the Multi-Model-Container.
6. This Multi-Model-Container is transferred to the actor.

4 Related work

The common standardised access model role-based access control model (RBAC) [9] is based on the concept of the user role as an intermediary between subjects and permissions and is purely subject-based. The properties of the objects have no effect on the access decision. Therefore, role assignments may be wrong after a state change of the entities (objects as well as subjects). Various proposals have extended the RBAC model with attribute-based access control capabilities [17] which also consider environment attributes (e.g. system status, time, date), subject attributes (e.g. age, location, proofs of identity) as well as object attributes (e.g. size, value, location, state of objects). Priebe et al. [18] proposes an attribute-based access control approach, but roles are subject-dependently modelled. Kumar et al. use in [19] context filters for role assignment, based on hash tables describing user context and object context-attributes. Franzoni et al. presents in [16] a fine-grained access control model, with focus on Semantic Databases, using ontologies to describe the subject-object relationships. Last but not least, Goslar describes a context model with dynamic real-world object linking in an economic focus [13]. Common to all these approaches is an attribute based assignment of subjects to roles while the roles-permissions assignment remains static.

5 Outlook

It has outlined an approach which covers the aspects mentioned in chapter 1: (A1) Due to one filter of the Multi-Model-Container, the communication between the partners was simplified and accelerated. Example, it is now possible to use Multi-Model-Container also on mobile devices. (A2) Only those application models necessary for the current processing situation were transferred to the Multi-Model-Container. (A3) The transferred application models have the exact resolution (size) needed for further processing.

Both the major components of the filtering services as well as most of the required multi-model templates are still under development, making the approach only roughly sketched. Currently in the focus of the research at the TU Dresden are the methods for the generation of geometric partial models and scheduling time spans.

Another development is focused on the filtering of MMC for transitive object properties of model elements. An example scenario for this comes from subsequent processing. Here, the complete reduction of MMC to a supplementary multi-model is desired which contains only subsequent positions in the application model specifications, corresponding to a reduced geometry and link model. Such application model sections, due to the dynamic component, cannot be generated with template models.

References

- [1] MOESLEIN K., (2001): *Die virtuelle Organisation: Von der Idee zur Wettbewerbsstrategie*, In: Rohde, Markus , Rittenbruch, Markus , *Auf dem Weg zur virtuellen Organisation* , Physica-Verlag Heidelberg.
- [2] FISCHER K., (2007): *Intelligente Agenten für das Management virtueller Unternehmen*, In: *Information Management* 1/96, Computerwoche Verlag GmbH, Muenchen.
- [3] KELLER M., (2007): *IT supported co-operation in construction projects*, PhD thesis *Berichte des Instituts fuer Bauinformatik* , Heft 6, 978-3-86780-004-4
- [4] KOECHENDOERFER B., LIEBCHEN J.H., VIERING M.G., (2006): *Projektorganisation - Bau-Projekt-Management*, Teubner, 978-3-8351-9075-7
- [5] EASTMAN C. M., (1999): *Building Product Models: Computer Environments, Supporting Design and Construction*, Crc Pr Inc., 0849302595
- [6] FUCHS S., KATRANUSCHKOV P. and SCHERER R. J., (2010): *A framework for multi-model collaboration and visualization*, In Proc. ECPPM 2010, Cork, Rep. of Ireland, Taylor and Francis, UK
- [7] KATRANUSCHKOV P., WEISE M., WINDISCH R., FUCHS S. und SCHERER R. J. , (2010): *Bim-based generation of multi-model views*, In Proc. CIB W78 2010.
- [8] CAMARINHA-MATOS L.M., AFSARMANESH H., (2008): *On reference models for collaborative networked organizations*, In *International Journal Production*, Vol. 46, No 9
- [9] FERRAILOLO D. F., J. A. C., KUHN D. R., (1995): *Role-based access control (rbac): Features and motivations*, In *Proceedings of 11th Annual Computer Security Application*.
- [10] SOHR K., DROUINEAUD M., AHN G.-J., (2005): *Formal Specification of Role-based Security Policies for Clinical Information Systems*, In *Proceedings of the 2005 ACM symposium on Applied*, doi:10.1145/1066677.1066756.
- [11] HILBERT F., KATRANUSCHKOV P. and SCHERER R. J., (2010): *Formal Fine-Grained Information Access in Virtual Organisations*, In Proc. eChallenges e-2010 Conference, 27-29 October, Warsaw, Poland, IIMC International Information Management Corp. Ltd., Dublin, Ireland.
- [12] SALTZER J. H., SCHROEDER M.D., (1975): *Protection of Information in Computer Systems*, In *Proceedings of the Ieee*, doi:10.1109/PROC.1975.9939.
- [13] GOSLAR, K., (2006): *Ein Integrations- und Darstellungsmodell für verteilte und heterogene kontextbezogene Informationen*, PhD Theses.
- [14] HORROCKS I., PATEL-SCHNEIDER P.F., BOLEY H., TABET S., GROSOFF B. and DEAN M., (2004): *SWRL: A Semantic Web Rule Language Combining OWL and RuleML*, In *W3C Member Submission*,.
- [15] SCHOLZ C., (1994): *Die virtuelle Organisation als Strukturkonzept der Zukunft?*, in *Diskussionsbeitrag Nr. 30 des Lehrstuhls für Betriebswirtschaftslehre*, Universität des Saarlandes Saarbrücken.
- [16] FRANZONI S., MAZZOLENI P., VALTOLINA S., BERTINO E., (2007): *Towards a Fine-Grained Access Control Model and Mechanisms for Semantic Databases*, In *Web Services, 2007. ICWS 2007. IEEE International Conference*, pp. 993 - 1000, doi:10.1109/ICWS.2007.176.

- [17] YUAN E. and TONG J., (2005): *Attributed based access control (ABAC) for web services*, In *IEEE International Conference on Web Services, Vols 1 and 2, Proceedings, 2005*, pp. 561-569, doi:10.1109/ICWS.2005.25.
- [18] PRIEBE T., DOBMEIER W. and KAMPRATH N., (2006): *Supporting attribute-based access control with ontologies*, In *Proc. 1st Int. Conf. on Availability, Reliability and Security, 2006*, pp. 465472, doi:10.1109/ARES.2006.127.
- [19] KUMAR. A, KARNIK N. and CHAFLE G., (2002): *Context Sensitivity in Role Based Access Control*, In *ACM SIGOPS Operating System Review 36(3)*, vol. 36, 2001, pp. 53–66, doi:10.1145/567331.567336.